Strategy Research Project

Cyberspace: Regional and Global Perspectives

by

Colonel Brett Reister
United States Army

United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
2012

2. REPORT TYPE
Strategy Research Project

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

Cyberspace: Regional and Global Perspectives

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Brett Reister

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Mr. William Waddell
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution: A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

As the newest war-fighting domain, cyberspace, and the authorities, roles, and responsibilities associated with it, continue to cause confusion despite concerted efforts of clarification. Significant friction exists between the geographic combatant commands, specifically responsible for operations within their theater, and the newly established United States Cyber Command (USCYBERCOM), the sub-unified command responsible for the global defense and operations in and through this critical domain. Acknowledging the cyberspace domain exists without regard to geographic boundaries, who is in charge of operations in and through this domain and when? Examining proposed options and perspectives for command and control are necessary to determine the right balance to achieve unity of command and unity of effort in a global domain with regional implications.

15. SUBJECT TERMS
Cyber, Domain, Authorities, Command and Control, USCYBERCOM, Geographic Combatant Commands

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

CYBERSPACE: REGIONAL AND GLOBAL PERSPECTIVES

by

Colonel Brett Reister
United States Army

Mr. William Waddell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Brett Reister

TITLE: Cyberspace: Regional and Global Perspectives

FORMAT: Strategy Research Project

DATE: 22 February 2012 WORD COUNT: 5,704 PAGES: 30

KEY TERMS: Cyber, Domain, Authorities, Command and Control, USCYBERCOM, Geographic Combatant Commands

CLASSIFICATION: Unclassified

As the newest war-fighting domain, cyberspace, and the authorities, roles, and responsibilities associated with it, continue to cause confusion despite concerted efforts of clarification. Significant friction exists between the geographic combatant commands, specifically responsible for operations within their theater, and the newly established United States Cyber Command (USCYBERCOM), the sub-unified command responsible for the global defense and operations in and through this critical domain. Acknowledging the cyberspace domain exists without regard to geographic boundaries, who is in charge of operations in and through this domain and when? Examining proposed options and perspectives for command and control are necessary to determine the right balance to achieve unity of command and unity of effort in a global domain with regional implications.

CYBERSPACE: REGIONAL AND GLOBAL PERSPECTIVES

> Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space.
>
> —2010 Quadrennial Defense Review[1]

Cyberspace is the newest war-fighting domain and is the only man-made domain. Because of the different man-made limitations, and conversely the lack of physical/geographic limitations imposed on it, this domain remains quite distinct and unique from the other domains of land, air, sea, and space. Does this distinctness require a unique command and control structure containing unique authorities? Cyberspace transcends the normal geographical boundaries and typical time span relationships which characterize the physical domains. However, because it resides on, in, and through all the physical domains, the ability to command and control and retain specific authorities must have some of the same characteristics as that which exists on land, air, sea and in space. The requirement to manage, coordinate, and control actions in cyberspace does exist, and therefore a viable structure with clearly understood roles and authorities must be established.

The 2011 Unified Command Plan assigns specific cyberspace responsibilities to the Commander of United States Strategic Command (STRATCOM), to include: direct the operation and defense of DoD networks, plan against cyberspace threats, coordinate with combatant commands and other US government agencies when cyberspace effects cross geographic areas of responsibility, coordinate the integration of theater security cooperation cyberspace related activities with geographic combatant commands, and execute directed cyberspace operations. The same Unified Command

Plan directs geographic combatant commands to execute authority over missions and assigned forces within their AORs, leading to uncertainty among the combatant commands about command and control relationships for operations in cyberspace.[2]

Establishing clear roles, responsibilities, and command relationships in this rapidly evolving, growing, and operating domain is apparently a challenging task. Despite several GAO reports finding necessity to clarify authorities and command and control relationships, there remains frustration and confusion across the Department of Defense as to who is in charge of what and when in cyberspace.[3] One report states, “Without complete and clearly articulated guidance on command and control responsibilities that is well-communicated and practiced with key stakeholders, DoD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyber operations.”[4] There also exists no specific joint doctrine which adequately address operations in cyberspace, merely a joint test publication with no current indication of when it will be finalized.[5]

Though cyberspace exhibits characteristics of the other physical domains, of which there are largely clear lines of authority and responsibility, it is also clearly different. The geographic combatant commands have an obvious stake in what goes on within their area of responsibility, to include cyberspace related operations/events. Arguments exist for the combatant commands to exercise a large role in controlling cyberspace operations within their boundaries. Others contend United States Cyber Command (CYBERCOM) should have primacy due to the global nature of the cyber domain and the simple fact that these operations do not recognize boundaries. There are other options proposed creating functional-like relationships, service-like relationships and combinations of both. Many would argue there is no, “one size fits all” command and control relationship for cyberspace. In contrast, there can be standard relational authorities implemented to clarify roles and responsibilities without leaving it up to the individual services or units to interpret. It merely requires an approved doctrinal template for units, services and organizations to follow and subsequently to be enforced.

In order to address this command relationship issue, an obvious question must be asked. Is this command and control realm in cyberspace that different from the other domains in respect to authorities and responsibilities? After all, what was the need to create a sub-unified command if not to standardize processes, establish authorities and maximize efficiencies? Each geographic combatant command has a slightly different perspective on how their cyberspace relationships function, operate, and interact. It should not be this way. The responsibilities and authorities should be the same without regard to geographic location. A standard set of procedures with a clear understanding of roles, responsibilities and authorities is necessary to function effectively in this environment, the same as any other.

This paper will examine perspectives and options of command and control relationships, roles, responsibilities and authorities, in cyberspace, among the geographic combatant commands (GCCs) and CYBERCOM.

<u>Framing the Environment</u>

Examining the command relationships and authorities of cyberspace first requires an understanding of how this domain is defined. There are several recent definitions which are widely accepted by government and the DoD. In 2008, Deputy

Secretary of Defense Gordon England defined cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunication networks, computer systems, and embedded processors and controllers."[6] Some argue this definition is missing a key component by failing to identify the "unique and defining" characteristics of cyberspace. After all, it is the only domain which cuts across all other physical domains simultaneously and with unmatched speed. Perhaps a more descriptive definition is offered by Dr. Daniel Kuehl, defining cyberspace as, "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." Whatever definition used, it is important to understand the cyberspace domain is more than just computers and information, and these related networks are found in both the physical and virtual world, as well as inside and outside geographical boundaries.[7] An additional key component to these definitions could include those that operate in, on and through this environment.[8]

The 2011 National Military Strategy (NMS) confirms cyberspace as a war-fighting domain that enables effective war-fighting in the other physical domains. The NMS further recognizes cyberspace capabilities as an enabler to the GCCs, effectively identifying it as a supporting effort to the GCCs. It also specifically directs STRATCOM and CYBERCOM to collaborate with other government agencies, non-government players, and international participants in order to "develop new cyber norms, capabilities organizations and skills."[9] Development of an effective range of options is recognized as necessary to counter extensive attacks and intrusions. There is also a telling statement which admits a shortcoming in cyberspace authorities and command relationships, identifying the need to gain executive and legislative decisions to establish and clarify authorities required for effective operations in cyberspace. The Chairman's main visionary document, which provides the ways and means by which the military will advance national interests identifies primacy of support to the GCCs and at the same time exposes a lack of clarity in command and control authorities. A requirement that remains unfulfilled.[10]

<u>Cyberspace Background and Challenges</u>

The Department of Defense acknowledges dependence on cyberspace to function, stating clearly, "DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."[11] CYBERCOM was created to focus the department's efforts and meet emerging requirements in this vital domain.

CYBERCOM became fully operational capable (FOC) on October 31, 2010, as a sub-unified command under USSTRATCOM. It accomplished this by merging two legacy organizations, Joint Functional Component Command-Network Warfare (JFCC-NW) and Joint Task Force-Global Network Operations (JTF-GNO). Co-locating at Fort Meade, Maryland, with the National Security Agency (NSA) enabled leveraging of technical capabilities, strengthened partnerships between the offensive and defensive functions on the Department of Defense Global Information Grid (DoD GIG), and established unifying command and control over both mission sets. Other activities achieved to make CYBERCOM FOC included assigning service cyber components to

STRATCOM, initial efforts were implemented to provide support to the combatant commands including establishing processes to identify cyber support requirements.[12]

CYBERCOM's mission is to plan, coordinate, integrate, synchronize and conduct activities to direct the operations in defense of specified DoD information networks and be prepared, when directed, to conduct full spectrum military cyberspace operations to enable actions in cyberspace, and deny the same to our adversaries.[13] CYBERCOM's mission requires balance to address the growing threat from highly capable adversaries, while simultaneously ensuring uninhibited mobility in cyberspace for the United States and its allies, within both civilian and government sectors (including the military).[14] DoD's networks provide great advantages to the force, but are vulnerable to attack and degradation. The United States military has come to expect rapid, assured and protected information flow to conduct the full range of military operations required to defeat an adversary. Protecting and leveraging over seven million computers across fifteen thousand networks is an enormous responsibility. In numerous venues, General Keith Alexander, the commander of CYBERCOM, acknowledged the requirement for close collaboration and clearly understood roles and responsibilities, including those within DoD's primary network communications service provider, the Defense Information Systems Agency (DISA).[15]

CYBERCOM's service components are the action arm of the command, executing and implementing its directives and plans. This assigned relationship provides coordinating effects from CYBERCOM to the services. It does not clarify roles and responsibilities among the geographic combatant commands, where the war-fighting occurs. General Alexander also recognized this requirement with on-going efforts to increase and improve interaction with and clarify supported/supporting relationships with the combatant commands. Furthering USCYBERCOM's supporting role, he also clarifies the command's mission of conducting full spectrum military operations to enable actions in all domains. One of the stated goals is to work with the combatant commands to synchronize plans and processing efforts to provide the joint effects required.[16]

Perceptions exist, however, of a cultural divide within the cyberspace community. There seem to be two camps, even after progress was made consolidating functions to achieve unity of effort. Despite the consolidation of JTF-GNO (which handled the protect and defend aspect of DoD networks and cyberspace) and JFCC-NW (which handled the attack and exploit aspect of cyberspace) beneath CYBERCOM, the divide remains. This gap is characterized by two separate and distinct focus areas, one on achieving offensive effects, the other on facilitating operational effectiveness and protection of DoD's current network architecture. This cultural divide between the attackers and defenders often causes the two camps to talk past each other, creating a disconnect in overall dialogue about cyberspace roles, functions, responsibilities and authorities. The communications community is largely focused on providing, operating, maintaining and defending DoD's networks, while many in the intelligence/operations community view attack and exploit efforts with primacy. Identifying clear responsibilities, authorities and coordination lines, integrating and truly consolidating both aspects of cyberspace will help bridge this cultural divide and facilitate the goal of cyber situational awareness offensively and defensively[17]

Offensive and defensive cyber situational awareness and integration is necessary to achieve operational and national strategic objectives. The protection, defense and maintenance of our critical networks and maintaining cyberspace freedom of movement is a key component for more than just the military. Civilian and other government communities, as well as partners and allies, absolutely rely on this open and protected domain. The president recently discussed this importance in the International Strategy for Cyberspace Operations. President Obama recognized the increasing need for reliable and secure networks, the necessity to build and enhance alliances to effectively address cyber threats, and the requirement to expand cooperation to increase collective security.[18]

Additional policy continues to emphasize shoring up defensive postures on DoD's information systems and networks. The DoD Strategy for Operating in Cyberspace focuses on cybersecurity and enumerates strategic initiatives to achieve national security objectives, defend national interests and effectively operate in the cyberspace domain. These initiatives build on and reinforce the president's International Strategy for Cyberspace, and focus DoD's strategic efforts for operating in cyberspace. In addition to guidance on viewing cyberspace as an operational domain, strategy initiatives center on defensive concepts to protect DoD networks, partnerships to facilitate a whole of government cybersecurity strategy, and building allied relationships to improve collective cybersecurity.[19] The priorities identified in these guiding policy documents clearly illustrate the critical requirements for, and importance of an effective cyberspace posture capable of integrated full spectrum cyberspace operations.

United States Central Command

In many instances the GCCs must have a measure of operational command and control of cyberspace to support operational priorities in their area of responsibility (AOR). The framework, supporting multiple networks, validates this requirement. United States Central Command (CENTCOM) is a prime example of this necessity, operating on 26 networks, 24 of which are outside the scope of CYBERCOM's responsibility. These other networks include classified (at various levels), unclassified, and multiple coalition networks. At the Combined Joint Task Force (CJTF) level, within the CENTCOM theater of operations, there are even more networks beyond the purview of their own GCC. Due to the operational complexities of numerous United States and coalition networks, and the requirement to enable subordinate commands to include existing and future CJTF's, CENTCOM recommends a hybrid approach to cyberspace command and control, incorporating both GCC and service cyber component command authorities. In their view, this flexible hybrid approach would enable identification of the best means of support based on specific mission requirements. This would also allow determination of which mission sets are best executed at which level. [20]

To support these varied "mission threads," CENTCOM recommends establishing a Regional Cyber Center (RCC) to synchronize and integrate cyber force actions across the breadth of the domain, beyond just NIPR and SIPR, and including the various Joint Operational Areas (JOAs) in the AOR. Standing up centers instead of specific functional commands, would also achieve unity of effort among key operational, intelligence, and communications functions. This could provide more effective coordinated synergy among the cyberspace functions ranging from attack and exploit to provide and defend.

CENTCOM also posits that the command and control of cyberspace should begin with the war fighting commander's assessment and determination of appropriate missions and authorities at each echelon. Requirements should be identified based upon the specific mission followed by allocation of resources with logically associated command relationships (supporting/supported). The goal for this cyberspace command and control construct is a unified response and a shared awareness covering the full spectrum of cyber operations – provide, defend, attack and exploit.[21]

United States European Command

United States European Command's (EUCOM) perspective on command and control of cyberspace is one focused more on achieving/controlling effects in the EUCOM AOR through cyberspace operations than specific command and control of cyber assets and organizations. EUCOM has a cyberspace command and control construct with overall purview at the general officer level. The dual-hatted Deputy J3, (Brigadier General) functions as the director of the Joint Force Cyber Center (JFCC) and EUCOM Cyber Integration (ECCI) Center. This construct effectively unifies the intelligence, operations and plans efforts with the information technology and C4 support (traditional communications) sections, and a cyber engagement section, which facilitates international/NATO engagement and coalition C4 interoperability. Within this construct, EUCOM looks to integrate CYBERCOM's Cyber Support Element (CSE) and DISA's Theater Network Operations Center within the JFCC Operations and Plans Divisions.[22]

EUCOM recognizes and embraces cyberspace as a war fighting domain, however, having no specific functional component command with overall purview or responsibility for the assets that function in the cyber domain, unlike the other physical domains (such as a Joint Force Air Component Command (JFACC) or Joint Force Maritime Component Command) or a service component command (such as United States Air Forces Europe (USAFE)), prompts the command to view and treat cyberspace as an enabling function focused on achieving effects in the other domains. This cross-cutting concept and perspective relieves pressure on a "cyber boss" to achieve effects in isolation, integrating efforts across the staff and within other domains. By virtue of the inherent regional perspective, EUCOM maintains a primary interest in the partnered relationships developed within the theater and how the functions/domains can enhance their relationships.[23]

As CYBERCOM is globally focused, and the GCCs remain AOR focused, EUCOM's perspective is similar to other GCCs in the primacy of situational awareness within the theater. This is particularly true when a subordinate JFC (Joint Force Commander) or JTF is employed to conduct operations. It is difficult, if not impossible, for those outside the AOR to recognize in entirety, the scope of the operational imperatives and lines of effort a commander in a specific operational area deems critical. This fact alone lends credibility to a certain aspect of cyberspace operational "trigger control," for lack of a better term, in regards to effects in an AOR. This does not require complete control of cyberspace assets but does necessitate AOR control of execution directive in order to meet a forward commander's requirement synchronized with operational objectives. The idea is CYBERCOM executes the mission with their assets but the GCC/JFC (forward)/JTF Commander controls the timing of execution, achieving the desired effects in requisite time and space. The focus is on the effects, and coordination across functions and domains, not on who executes or owns the assets.[24]

United States Pacific Command

Illustrating the importance of operating, securing, and controlling cyberspace, Admiral Willard, the Commander of United States Pacific Command (PACOM), warned during a security conference in Hawaii, military networks could be rendered completely inoperable in wartime if cyberspace operators do not have situational awareness of what is happening inside this domain. Emphasizing the importance of command and control within cyberspace, he stated, “in command and control, you can’t control what you can’t see, and you must be able to control everything in these domains.” He further stated, “You can’t control that domain unless you can see into it, sense inside it and control it.”[25]

To meet PACOM’s command and control requirements for cyberspace and cyberspace operations, objectives were established by the command. The first, and main objective is to enable the GCC commander to command and control this domain within his AOR similar to the other physical domains. Subsequent objectives include: facilitate GCC mission-risk decision making in the cyber domain in support of assigned missions, and synchronize cyber operations regionally, nationally and with allies in the AOR. Further, PACOM’s intent for a viable cyber command and control structure would be one which mirrors the operational chain of command, is scalable, operates across the CYBERCOM lines of operation (DGO-DoD Global Information Grid Operations, DCO-Defensive Cyberspace Operations, OCO-Offensive Cyberspace Operations) allowing consolidation of GCC cyber expertise from across the GCC staff, and promotes unity of effort among associated organizations within the theater. These efforts look to establish a central entry/exit point for cyberspace issues within the AOR, as well as directing the operational cyber effects in support of both GCC and established joint task forces.[26]

United States Southern Command

Every geographic combatant command has unique considerations when operating in the cyberspace domain. United States Southern Command (SOUTHCOM) is no exception. SOUTHCOM also has similar perspectives as the other geographic combatant commands in regards to striking the right balance of cyberspace roles, responsibilities and authorities. Despite clear recognition of cyberspace being a global domain, there remains a prevailing thought of cyberspace capabilities and authorities existing within the GCCs to conduct cyberspace operations within their defined boundaries, granted the effects remain in the designated AOR. Even operating solely within the AOR, acknowledged coordinating efforts would be required between CYBERCOM and the GCC to ensure unity of effort.[27]

Upon implementation, SOUTHCOM's operational cyberspace effects would be conducted and/or coordinated from a Joint Cyber Center joined with SOUTHCOM's Joint Operations Center, attaining operations and intelligence synergy similar to other kinetic and non-kinetic operations currently occurring in other domains. In order to meet this vision, SOUTHCOM must overcome some additional challenges. Unlike the other GCCs, the initial integration effort of resourcing a cyber support element (CSE) to assist with cyberspace operations and global integration in each AOR has not been realized in SOUTHCOM. Lack of resourcing prompted the GCC to begin its own efforts to achieve desired cyberspace effects which could ultimately have unintended consequences across the DoD GIG. Without the required CYBERCOM coordination elements in place or being resourced like other GCCs, SOUTHCOM could become the weakest link in the global DoD network, exposing critical vulnerabilities to our adversaries or criminal elements.[28]

SOUTHCOM has the same general responsibilities in accordance with the UCP, however, its focus and methods of conducting operations differ from other GCCs, based on the AOR specific threat and environment. Cyberspace operational focus differs as well. The threats in the SOUTHCOM AOR are largely related to transnational actors and organized crime. Coupled with this threat is the major mission set of humanitarian assistance and disaster relief. The AOR specific threats and predominant operational environment often place SOUTHCOM in a supporting role to law enforcement and other interagency partners. Due to the varied focus, the targeting process for attaining effects is likewise modified. The same modification occurs in the cyberspace domain and becomes essentially a counter-targeting or defensive effort to protect key strategic assets or infrastructure in the AOR (i.e. the Panama Canal), vice employing offensive cyberspace operations.[29]

Despite the AOR specific aspects of SOUTHCOM, the GCC still expects to exercise some measure of authority over cyberspace effects specifically in the SOUTHCOM AOR. SOUTHCOM also concedes the necessity for coordination efforts with a resourced cyber support element, and ultimately relinquishing operational control to CYBERCOM when cyberspace operations reach and/or have impacts beyond the AOR.

Possible Options for Cyber Command and Control

Proposals exist to model the command and control of cyberspace after several existing command relationships. Hybrid solutions were also proposed in recognition of the uniqueness of this global domain. There are wide ranging perspectives on who should command, control, coordinate, train, and resource cyberspace forces, effects and operational capability. While much of the manning, training, and equipping function of cyberspace forces is provided by the services, there remains confusion on the overall responsibilities of the remainder of the operational functions. Who is in charge, when, and in what capacity? It is clear the geographic combatant commands have a dog in this fight being responsible for operations conducted within their AOR. CYBERCOM clearly has a role in ensuring operational capability of the DoD GIG, and executing full spectrum cyber operations to help maintain friendly freedom of movement in all the domains. The following options are ways to achieve the overall endstate of effectively coordinated and conducted cyberspace operations with identified authorities, responsibilities and command relationships.

One option proposed by some in the cyberspace community is commonly referred to as the USSOCOM (United States Special Operations) model. This model is based on the similarities of the Special Operations Forces (SOF) community in regards to its unique aspects and the need to create a special command structure to meet mission requirements. Cyberspace similarities to SOF include capabilities from all services, the combination of global and regional missions, and the requirement for a specific command to accomplish a unique mission set.[30] This model incorporates a Regional Cyber Commander (RCC) similar to a Theater Special Operations Command

(TSOC), maintaining the COCOM (Combatant Command) command relationship with the GCC. The RCC's responsibilities would include coordinated effects planning to support the GCC's focused operational plans, and function as the primary coordination point with CYBERCOM to facilitate global deconfliction of cyber operations. This model would grant OPCON (Operational Control) of the service provided networks to the RCC, exercising decision-making authority over the GCC networks. In this model, CYBERCOM's role would include manning, training, and equipping the cyber forces in each of the GCC's and would maintain responsibility over cyberspace operations which transcend GCC boundaries. The primary relationships established in this construct would be coordination authority between RCC and CYBERCOM and a supported/supporting relationship depending on where the operation/threat occurred. This model would also require CYBERCOM to reinforce the regional cyber forces in support of a JTF led operation in a particular AOR. A JTF Cyber Force could be established subordinate to the RCC and TACON to the JTF. Within this construct, cyber support elements, linked to specific components, would be established to ensure integration across all the domains. This model is an advantage from the GCC's perspective as it preserves unity of command within the specified AOR, allowing ease of integration with the other domains regionally. It is also argued this model supports the theory of treating cyberspace effects the same as other kinetic or non-kinetic effects, easing overall coordination and integration efforts.[31]

A disadvantage of the USSOCOM model is the simple fact that most cyberspace operations do not take place within a single GCC, minimizing the need for a formal RCC which could be underutilized. Additionally, the mere global nature of the domain, includes potentially vast consequences when executing certain specific operations. This reality could force authorities to remain at the CYBERCOM level, minimizing the need for a specific command structure at the GCC. Establishing a RCC to conduct and control these types of operations could also be a costly and resource intense endeavor. Finally, though unity of command and unity of effort may be achieved within a specific command structure and regionally, this construct could actually unhinge the overall cyberspace unity of effort due to the lack of functional alignment, creating a potential disconnected inefficiency with global cyberspace operations.[32]

A second potential option proposed is the USTRANSCOM (United States Transportations Command) model. This model employs a centralized command and control structure associated with USTRANSCOM's OPCON of global transportation assets, relinquishing control only when assets are physically retained within a GCC's boundary and used internally inside a particular AOR. This centrally controlled model facilitates flexibility at the strategic level allowing management of global assets to meet global priorities. Applying cyberspace to this construct includes a Joint Cyber Synchronization Center (JCSC), similar to CENTCOM's proposal, assigned to the GCC with a coordination relationship with CYBERCOM. This model conducts normal steady state operations within the theater through the Theater Network Operations and Security Center (TNOSC), the existing organization primarily responsible for operation, maintenance and defense of the regional network and information system assets. CYBERCOM would support operations from the offensive (attack and exploit) aspect with coordination being conducted through the JCSC.

During a contingency operation, this construct proposes standing up a JTF-Cyber element, with CYBERCOM maintaining combatant command authority, in support of an operational JTF. This would allow leveraging of offensive capabilities in support of both JTF and GCC objectives. The GCCs would maintain TACON of the service provided networks (operation and maintenance) with the more sophisticated technical capabilities centrally controlled at CYBERCOM. This centralized command and control structure is an advantage from the strategic perspective, providing a large measure of flexibility to employ limited assets. An additional advantage is centrally locating the assets, capabilities and personnel with the headquarters (CYBERCOM or CYBERCOM controlled [JTF-Cyber]) retaining authority for operations, and ultimately providing unity of command at the strategic/global level.[33]

The disadvantages identified in this model are the lack of unity of command at the GCC level and a decreased unity of effort during contingency operations. The arguments made against this model point out the dissimilar nature of global transportation assets with the requirement to integrate cyber effects at the operational and tactical level, in the cyber domain as well as the physical domains. Having a globally centralized authority controlling these effects within a GCC's AOR could become disjointed from regional operational necessities, hampering unity of effort.

An additional middle ground approach was also proposed; one which allows CYBERCOM to maintain some centralized control while effectively supporting GCC's forward regional planning and execution efforts. This model, known as the hybrid model, blends aspects of the USSOCOM model and USTRANSCOM model. The hybrid command and control structure allows for a regional CYBERCOM presence, a Regional

Cyber Center (RCC), with COCOM authority to CYBERCOM for global cyberspace operations and operations occurring outside the AOR that potentially impact the GCC, and TACON authority to the GCC for regionally focused matters. The RCC's primary focus would be on integration efforts to support the GCC. TACON of the RCC could also be rescinded to CYBERCOM if necessary to handle cross boundary operations.[34]

During contingency operations, the hybrid model provides augmentation to a JTF from CYBERCOM, standing up a JTF-Cyber component with an OPCON relationship with CYBERCOM (for global integration/considerations) and a TACON relationship with the GCC. The JTF-Cyber component would again be focused on integration of cyber effects in support of the operational JTF while simultaneously maintaining global situational awareness and deconfliction of operations with CYBERCOM. This model assumes cyberspace exploit and attack authority will remain with CYBERCOM allowing for unity of command at the functional level.[35]

The identified drawbacks to this model include additional manning requirements in an already critically constrained function, and a potential lack of confidence in the support of GCC priorities and required effects by CYBERCOM in a timely manner, caused by a weak command link to the GCC. The hybrid model attempts to provide centralized command and control in support of the global cyberspace mission (USTRANSCOM model) and a more specific functional command structure to support GCC requirements. The ultimate goal is to provide measured unity of command and unity of effort to attain effects globally and regionally.[36]

One of the current arguments for centralized control of cyberspace effects likens cyberspace to the air domain. Limited, powerful and highly sought after air assets are centrally controlled by a single air commander focused on the broader scope of an operation, more effectively arbitrating competing tactical support demands against strategic and operational necessities.[37] The parallel cyberspace argument states, because cyberspace is a truly global domain that literally moves at the speed of light, it should be controlled centrally by a cyber operator at a cyber command with a global perspective.[38]

The counterargument is air and cyberspace characteristics are not that similar. Though a need exists to have a global perspective, there is less of a limit on asset management. This argument confuses limited asset management with effects – a desired outcome from a specific action. When addressed in its entirety, cyberspace is not overly constrained by devices/equipment and does not equate to air power in this perspective. Effects are achieved at many levels in cyberspace and can subsequently be managed, coordinated, supported, and controlled at many levels. There is a clear need for coordinated efforts as actions can have global effects, however regional situational awareness is often achieved at the AOR level with designated responsibilities and authorities granted to achieve a GCC's or JFC's desired effect as the supported war fighter. Many GCCs contend, a cyberspace operator at a cyber headquarters thousands of miles away will likely not understand the operational requirements necessary for integrated success in a particular JOA, let alone understand the local or regional commander's intent. There must be established, coordinated relationships to allow flexibility at the Joint Force Commander level while simultaneously protecting strategic/global interests. Similar to previously mentioned constructs, this could be achieved through a supporting relationship to a GCC with tactical control for operations within the AOR, while maintaining operational control of specific skill set cyberspace assets/personnel at CYBERCOM.[39]

Conclusion

Cyberspace command and control remains a challenge between STRATCOM/CYBERCOM and the GCCs. Achieving the necessary unity of command and unity of effort in this global domain that recognizes no boundaries, yet has impacts within and across specific regions requires coordination efforts similar to and different from other domains. Controlling cyberspace assets has wide ranging implications, constraints, and limitations. The uniqueness of this domain creates difficulty when trying to implement a traditional command and control structure with clear roles, responsibilities and authorities.

The most feasible cyberspace command and control construct to achieve measured unity of command and unity of effort while facilitating dual global and regional focus is a blended hybrid model of the SOCOM and TRANSCOM models, with some minor modifications gleaned from the GCC perspectives. Under this structure, Regional Cyberspace Centers (RCCs) within the GCCs would be responsible for synchronizing all aspects of cyberspace operations to include providing network services, defense of the DoD GIG, and conducting offensive cyberspace operations. The RCC would be co-located and integrated with the GCCs operations, intelligence, and plans functions to achieve synergy across the spectrum of operations. The GCC would maintain TACON of the RCC to allow for regional mission support and to achieve effects directed by the GCC and subordinate JFCs when employed. To meet the global support requirements of cyberspace operations, CYBERCOM would maintain an OPCON relationship with the

RCC to support cyberspace efforts which cut across GCC boundaries. Though unity of command suffers in this construct, it is unrealistic to expect a globally focused functional command not to exercise some level of control over assets and operations that traverse beyond numerous geographical boundaries.

Keeping the RCC as a directorate or center instead of a specific regional functional command organization also allows for ease of staff coordination internally within the GCC staff and externally with CYBERCOM. Additionally, it allows for construct modification if necessary to meet changing requirements in the future. A formal cyber command organization brings unnecessary command and staff baggage, would limit the flexibility to respond to changing requirements, and would likely disrupt the purpose of rapid and streamlined coordination in this dynamic environment.

Despite the challenges presented by this unique domain, effects must be achieved globally and regionally. Several proposed command and control constructs attempt to clarify command lines and supporting/supported relationships. Each has advantages and disadvantages. There is no perfect solution for this dilemma. Whichever command and control construct is ultimately decided, it must effectively address both global and regional realities. There must be a measured compromise to enable global capabilities to support regional priorities with regional situational awareness. There must also be an understanding of the global responsibility and boundary-less effects this domain permits. A balance must be struck to allow measured GCC prioritized effects to be achieved supporting the UCP directed AOR specific mission; along with similarly measured, consolidated, globally focused prioritized effects to be achieved in support of CYBERCOM's worldwide offensive and defensive mission as well.

No command and control construct will be ideal initially, and will likely require modification as requirements and the environment changes. However imperfect the determined command and control structure, it must be clear to those operating in, on or through this critical domain. Cyberspace transcends many traditional aspects in the physical and geographic world, but it still requires humans and forces to utilize it, and they must know what they can do on, in and through it, and when.

Endnotes

[1] Robert Gates, *Quadrennial Defense Review* (Washington, D.C.: Office of the Secretary of Defense, 1 February 2010), 37.

[2] Barrak Obama, *Unified Command Plan* (Washington, D.C.: The White House, 6 April 2011), 3-4.

[3] U.S. Government Accountability Office, *Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities* (Washington, D.C.: U.S. Government Accountability Office, May 2011), 19.

[4] U.S. Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities* (Washington, D.C.: U.S. Government Accountability Office, July 2011), 8.

[5] Ibid., 5.

[6] Gordon England, *Deputy Secretary of Defense Memorandum: The Definition of Cyberspace* (Washington, D.C.: Office of the Deputy Secretary of Defense, 12 May 2008).

[7] Daniel T.Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University, 2009), 28.

[8] Jeffrey L. Caton, "Emerging Challenges: Cyberspace and Cyberstrategy," lecture, U.S. Army War College, Carlisle Barracks, PA, November 15, 2011, cited with permission of Mr. Caton.

[9] Michael G. Mullen, *The National Military Strategy of the United States of America* (Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff, 8 February 2011), 9.

[10] Ibid., 9-10.

[11] United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: United States Department of Defense, July 2011), 1.

[12] Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 3-4.

[13] Ibid., 4.

[14] Ibid., 5.

[15] Ibid., 8.

[16] Ibid., 10.

[17] COL John Burger, U.S. Army, Chief, Cyber Security Division, U.S. Central Command, telephone interview by author, January 17, 2012.

[18] Barrak Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: The White House, May 2011), 20-21.

[19] *DOD Strategy for Operating in Cyberspace, 5-9.*

[20] COL John Burger, "Cyber Command and Control (C2): Enduring Cyberspace Operations Command and Control Framework," August 1, 2011, http://www.afcea.org/events/pastevents/documents/LWN11_Track_1_Session_3.pdf (accessed January 12, 2012).

[21] Ibid.

[22] LTC Paul Mullins, U.S. Army, EUCOM Cyber Integration Directorate, U.S. European Command, email, January 30, 2012.

[23] COL Charles Eassa, U.S. Army, former U.S. European Command J39, interview by author, Carlisle Barracks, PA, February 3, 2012

[24] Ibid.

[25] Robert Ackerman, "Cybersecurity Dominates Asia-Pacific Agenda," *Signal* 65, no. 5 (January 2011): 59.

[26] Col Doug Mason, U.S. Marine Corps, U.S. Pacific Command, Cyberspace Operations Center, e-mail message to author, January 24, 2012.

[27] COL Randy Taylor, U.S. Army, J6, U.S. Southern Command, telephone interview by author, January 29, 2012.

[28] Ibid.

[29] Ibid.

[30] David C. Hathaway, “The Digital Kasserine Pass: The Battle Over Command and Control of DoD’s Cyber Forces,” *Foreign Policy at Brookings* (Washington, D.C.: Brookings, July 15, 2011), 10.

[31] Ibid., 13.

[32] Ibid., 13.

[33] Ibid., 16.

[34] Ibid., 18-19.

[35] Ibid., 20.

[36] Ibid., 20.

[37] Ibid., 21.

[38] Ibid., 22.

[39] COL Burger, telephone interview by author, January 17, 2012.